

Officer or alternate. Such registering process shall include the recording of: The date the document was received and originated; the classification of the document; the number of copies; the title and description of the document; the disposition and date; the location of the document; and the serial number assigned to the document. For example, the 25th Top Secret document received within the Criminal Division during 1982 could be assigned the following Top Secret control number: CRM-82-0025.

(c) Top Secret accountability registers shall be maintained by each originating and receiving office for all Top Secret documents received or in its custody.

(d) The name and title of all individuals, including stenographic and clerical personnel, to whom information in Top Secret documents has been disclosed, and the date of such disclosure, shall be recorded. The use of a sheet of paper permanently attached to the document concerned may serve as a disclosure record or log for these purposes. Disclosures to individuals who may have had access to containers in which Top Secret information is stored need not be recorded on disclosure records. Disclosure records shall be retained for two years after the document concerned is transferred, downgraded or destroyed.

§ 17.112 Inventories.

Top Secret documents and material shall be inventoried at least once annually. Organizations which store large volumes of classified information may limit their annual inventory to documents and material which have been disclosed within the past year. If a storage system contains large volumes of information and security measures are adequate to prevent access by unauthorized persons, the head of the Office, Board, Division or Bureau may submit a request for a waiver of the annual inventory requirement to the Department Security Officer. However, the request must be fully justified to provide a basis for the Attorney General to approve, in writing, the waiver of these annual inventory requirements.

§ 17.113 Accountability of Secret and Confidential information.

Security Programs Managers within all Offices, Boards, Divisions, and Bureaus are responsible for ensuring that accountability procedures for Secret and Confidential information are established within their respective organizations. Such procedures shall be written and shall pertain to Secret and Confidential information originated or received by a Department component; distributed or routed to a subelement of such component; and disposed of by the component by transfer of custody or destruction. Copies of written procedures for the accountability and control of Secret and Confidential information shall be forwarded to the Department Security Officer. At a minimum, such procedures shall provide for the identification of the document.

§ 17.114 Accountability of reproduced documents.

Reproduced copies of Top Secret, Secret and Confidential documents are subject to the same accountability and controls as the original documents. (See § 17.100(b).)

§ 17.115 Working papers.

“Working papers” are classified documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be dated when created; marked with the highest classification of any information contained therein; protected in accordance with the assigned classification; destroyed when no longer needed; and marked with a declassification or review date when placed in permanent files. Working papers shall be accounted for and controlled in the manner prescribed for a finished document of comparable classification when released by the originator or transmitted through message center channels; filed permanently; or retained more than 180 days from date of origin.